UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ERICKSON J. OCASIO, Individually and on behalf of all others similarly situated,	)	**Case No. 1:19-cv-4989**
Plaintiff,	)	**Jury Trial Demanded**
vs.	)	
LABORATORY CORPORATION OF AMERICA HOLDINGS, d/b/a LabCorp,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Erickson J. Ocasio, on behalf of himself and all others similarly situated, through counsel, for his Complaint against Defendant Laboratory Corporation of America Holdings d/b/a LabCorp states:

1. This is a data breach class action on behalf of 7.7 million patients whose sensitive personal information was accessed by computer hackers in a cyber-attack (the "Data Breach"). Information compromised in the Data Breach includes Social Security numbers, financial information (*e.g.*, credit card numbers and bank account information), medical information, date of service, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), personal and medical information as defined in the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. 530/5, and additional personally identifiable information (collectively, "Most Sensitive Personal Information").

2. Plaintiff brings this class action lawsuit on behalf of a nationwide class and an Illinois statewide sub-class to address Defendant' negligent—indeed reckless—failure to use reasonable cybersecurity measures to protect class members' Most Sensitive Personal Information.

3. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[1] Cyber criminals can leverage Plaintiff's and class members' Most Sensitive Personal Information that was stolen in the Data Breach to commit thousands—indeed, millions—of additional crimes, including, opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

4. Because Defendant' presented such a soft target to cybercriminals, Plaintiff and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and class members must now and in the future closely monitor their financial accounts to guard against identity theft.

5. Plaintiff and class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

[1] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

6. Plaintiff seeks to remedy these harms on behalf of himself and all similarly-situated individuals whose Most Sensitive Personal Information was accessed during the Data Breach.

7. On behalf of himself and class members, Plaintiff seeks compensatory damages, statutory damages under the Illinois Personal Information Protection Act and Consumer Fraud and Deceptive Business Practices Act, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant' data security systems, future annual audits, and free credit monitoring services funded by Defendant, and other remedies as the Court sees fit.

PARTIES

8. Plaintiff Erickson J. Ocasio is an individual residing in Chicago, Illinois. He was a patient of LabCorp when LabCorp collected and received Plaintiff's Most Sensitive Personal Information in Illinois, which LabCorp maintained in its database. Based upon information and belief, including LabCorp's own Data Breach Notification Letter that Plaintiff received on July 12, 2019 (Attached as ***Exhibit A***), Plaintiff's Most Sensitive Personal Information was compromised in the Data Breach.

9. Defendant Laboratory Corporation of America Holdings d/b/a LabCorp (LabCorp") is incorporated in Delaware. Its principal place of business is in Burlington, North Carolina.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant conducts business in and throughout Illinois, Plaintiff and the class members provided LabCorp with their

Most Sensitive Personal Information in Illinois and that Most Sensitive Personal Information was used by Defendant to attempt to collect alleged medical bills inside the State of Illinois.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is a resident for venue purposes because it regularly transacts business here. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because all Defendant are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

13. LabCorp is one of the largest providers of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

14. LabCorp's invoices cover laboratory testing fees only and are separate from any bill received by a patient's physician. Patients can be charged by either directly going to a LabCorp facility or if their physician has sent their specimen to a LabCorp laboratory.

15. When certain LabCorp customers do not pay their invoices within the requested time period, LabCorp will reach out to a collection agency like Retrieval-Masters Creditors Bureau, Inc., d/b/a American Medical Collection Agency, Inc. ("AMCA").[2]

16. Upon information and belief, LabCorp would provide AMCA with LabCorp customers' Most Sensitive Personal Information, which AMCA subsequently housed in its own system, in order to facilitate collections. This information included first and last name, date of birth, address, phone number, date of service, provider, and balance information.

[2] AMCA filed Chapter 11 bankruptcy on June 17, 2019 (*In re: Retrieval-Masters Credit Bureau, Inc.*, U.S. Bankruptcy Court, S.D.N.Y., 19-23185) and is not joined as a party in this lawsuit.

17. On June 4, 2019, LabCorp publicly announced the following, in relevant part, in a Form 8-K filed with the Securities and Exchange Commission:

> According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp provided no ordered test, laboratory results, or diagnostic information to AMCA. AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers.

AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose Most Sensitive Personal Information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them.[3]

18. AMCA failed to properly safeguard class members' Most Sensitive Personal Information, allowing hackers to access their Most Sensitive Personal Information for eight months. AMCA also failed to properly monitor its systems. Had it properly monitored its systems, it would have discovered the intrusion much sooner than eight months after the breach began.

19. Defendant failed to properly monitor AMCA to ensure that proper data security safeguards were being implemented by AMCA throughout the breach period.

20. Upon information and belief, Defendant did not require AMCA to disclose its information security measures before entrusting AMCA with the Most Sensitive Personal Information of Plaintiff and class members. In short, Defendant handed off millions of individuals

[3]http://secfilings.nasdaq.com/filingFrameset.asp?FilingID=13474097&RcvdDate=6/4/2019&CoName=LABORATORY%20CORP%20OF%20AMERICA%20HOLDINGS&FormType=8-K&View=html (last accessed July 22, 2019).

Most Sensitive Personal Information to AMCA without taking adequate steps to evaluate AMCA's ability to protect that information as required by HIPAA and the Illinois Personal Information Protection Act.

21. Defendant had obligations created by HIPAA, the Illinois Personal Information Protection Act, industry standards, common law, and representations made to class members, to keep class members' Most Sensitive Personal Information confidential and to protect it from unauthorized access and disclosure.

22. Plaintiff and class members provided their Most Sensitive Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any business partners to which Defendant disclosed the Most Sensitive Personal Information would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. Indeed, Defendant promised patients that it would keep their Most Sensitive Personal Information confidential, stating in its Notice of Privacy Practices that it is "committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation."[4] Defendant's Notice of Privacy Practices also acknowledged that Defendant is subject to HIPAA.[5]

24. Defendant further stated in its Notice of Privacy Practices that its vendors maintain adequate data security over patient data, stating:

> LabCorp may disclose PHI to its business associates to perform certain business functions or provide certain business services to LabCorp. For example, we may

[4] *See* https://www.labcorp.com/hipaa-privacy/hipaa-notice-privacy-practices# (last accessed June 13, 2019).

[5] *Id.*

> use another company to perform billing services on our behalf. All of our business associates are required to maintain the privacy and confidentiality of your PHI.[6]

25. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach. The increase in data breaches and the attendant risk of future breaches were widely known to the public and to anyone in Defendant's industries, including Defendant.

Defendant's Data Security Failures and HIPAA Violations

26. Defendant's data security failures demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting patients' Most Sensitive Personal Information;

c. Properly monitoring its own data security systems for existing intrusions;

d. Ensuring that its vendors employed reasonable data security procedures;

e. Ensuring the confidentiality and integrity of electronic protected health information ("PHI") it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Implementing technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

---

[6] *Id.*

g. Implementing policies and procedures to prevent detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Protecting against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Ensuring compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

l. Training all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b).

Damages to Class Members

27. Plaintiff and class members have been damaged by the compromise of their Most Sensitive Personal Information in the Data Breach.

28. Plaintiff and class members face substantial risk of out of pocket fraud losses such as loans opened in their names, medical services billing their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

29. Plaintiff and class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and class members.

30. Plaintiff and class members have and may incur ongoing out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

31. Plaintiff and class members suffered a "loss of value" of their Most Sensitive Personal Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of "loss of value" damages in data breach cases.

32. Class members who paid Defendant for its services were also damaged via "benefit of the bargain" damages. Such class members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price class members paid to Defendant was intended to be used by Defendant to fund adequate data security and monitor its vendors' compliance with data security obligations. Defendant did not properly monitor its vendors' compliance with data security obligations. Thus, the class members did not get what they paid for.

33. Plaintiff and class members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

34. The U.S. Government Accountability Office noted in a report on data breaches (the "GAO Report") that identity thieves often use identifying data such as Social Security numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[7] As the GAO Report states, this type of identity theft is particularly harmful because it often

[7] *See* https://www.gao.gov/new.items/d07737.pdf (last accessed June 12, 2019).

takes time for the victim to become aware of the theft, and the theft can adversely impact the victim for years.

35. In addition, the GAO Report states that victims of identity theft may face "substantial costs and inconveniences repairing damage to their credit records."[8] identity theft victims are frequently required to spend many hours as well as money repairing the impact to their credit.

36. There may be a substantial time lag — measured in years — between when Most Sensitive Personal Information is stolen and when it is used. According to the GAO Report: "[O]nce stolen data have been sold or posted to the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[9] Thus, plaintiff and class members must vigilantly monitor their financial and medical accounts for many years to come.

37. With access to the type of information that was accessed in the Data Breach, criminals can use the information gained to gather additional information about Plaintiff and class members, open accounts in victims' names; receive medical service in the victims' name; obtain a driver's license or official identification card in the victim's name but with the thief's photo; use the victim's name and Social Security number to obtain government benefits; file a fraudulent tax return using the victim's information; and give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[10]

---

[8] *Id.*

[9] *Id.*

[10] *See* Federal Trade Commission, Warning Signs of Identity Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed June 12, 2019).

38. The Most Sensitive Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell it on the cyber "black-market" or "dark web" indefinitely. Cyber criminals routinely post stolen Social Security numbers, financial information, medical information, and other sensitive personal information on anonymous websites, making the information widely to a criminal underworld. There is an active and robust market for this information.

39. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionately higher numbers of data theft events than other industries. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

CLASS ACTION ALLEGATIONS

40. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a Nationwide Class defined as follows:

> All persons in the United States who utilized LabCorp's services and whose Most Sensitive Personal Information was maintained on AMCA's system that was compromised in the data breach announced by LabCorp on June 3, 2019.

and a Statewide Sub-Class defined as follows:

> All persons in the State of Illinois who utilized LabCorp's services and whose Most Sensitive Personal Information was maintained on AMCA's system that was compromised in the data breach announced by LabCorp on June 3, 2019.

41. Excluded from the above Classes are Defendant' executive officers, and the judge to whom this case is assigned.

42. **Numerosity**. The Classes are each so numerous that joinder of all members is impracticable. The Class consists of hundreds, if not thousands or more individuals, on information and belief.

43. **Commonality**. There are many questions of law and/or fact common to Plaintiff and the class. Common questions include, but are not limited to:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant owed a duty to class members to safeguard their Most Sensitive Personal Information;

d. Whether Defendant breached its duty to class members to safeguard their Most Sensitive Personal Information;

e. Whether computer hackers obtained class members' Most Sensitive Personal Information In the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiff and class members suffered legally cognizable damages as a result of Defendant's misconduct; and

h. Whether Plaintiff and class members are entitled to injunctive relief.

44. **Typicality**. Plaintiff's claims are typical of the claims of class members in that Plaintiff, like all class members, had his personal information compromised in the Data Breach.

45. **Adequacy of Representation**. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable counsel with significant experience in complex class action litigation. Plaintiff and his counsel are committed to

prosecuting this action vigorously on behalf of the Classes. Plaintiff's counsel has the financial and personnel resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to, or that conflict with, those of the Classes.

46. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and class members. The common issues arising from Defendant's conduct affecting class members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

47. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

48. Defendant has acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis under Fed. R. Civ. P. 23(b)(2).

COUNT I
NEGLIGENCE

49. Plaintiff realleges and incorporates by reference all preceding allegations.

50. Defendant required Plaintiff and class members to submit non-public personal information in order to obtain medical services, which it forwarded to AMCA for billing purposes.

51. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard class members' Most Sensitive Personal Information, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

52. Defendant owed a duty of care to Plaintiff and class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Most Sensitive Personal Information.

53. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between LabCorp and its client patients, which is recognized by laws and regulations, including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach.

54. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

55. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

56. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Most Sensitive Personal Information.

57. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect class members' Most Sensitive Personal Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Most Sensitive Personal Information;

b. Failing to adequately monitor the security of AMCA's networks and systems;

c. Failure to periodically ensure that its vendors, including AMCA, had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to class members' Most Sensitive Personal Information;

e. Failing to detect in a timely manner that class members' Most Sensitive Personal Information had been compromised; and

f. Failing to timely notify class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

58. It was foreseeable that Defendant's failure to use reasonable measures to protect class members' Most Sensitive Personal Information would result in injury to class members. Further, the breach of security was reasonably foreseeable given the known high frequency of data breaches in the medical industry.

59. It was therefore foreseeable that the failure to adequately safeguard class members' Most Sensitive Personal Information would result in one or more types of injuries to class members.

60. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

61. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

COUNT II
BREACH OF IMPLIED CONTRACT

62. Plaintiff realleges and incorporates by reference all preceding allegations.

63. When Plaintiff and class members provided their Most Sensitive Personal Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

64. Defendant solicited and invited class members to provide their Most Sensitive Personal Information as part of Defendant's regular business practices. Plaintiff and class members accepted Defendant's offers and provided their Most Sensitive Personal Information to Defendant.

65. In entering into such implied contracts, Plaintiff and class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

66. Class members were aware of, or reasonably anticipated that, Defendant would forward certain Most Sensitive Personal Information to vendors, as disclosed in Defendant's Notice of Privacy Practices.

67. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

68. Plaintiff and class members would not have entrusted their Most Sensitive Personal Information to Defendant in the absence of the implied contract between them and Defendant to keep the information reasonably secure. Plaintiff and class members would not have entrusted their Most Sensitive Personal Information to Defendant in the absence of Defendant's implied promise to monitor its vendors to ensure that they adopted reasonable data security measures.

69. Plaintiff and class members fully and adequately performed their obligations under the implied contracts with Defendant.

70. Defendant breached its implied contracts class members by failing to safeguard and protect their Most Sensitive Personal Information. Defendant breached its implied contract with class members by failing to properly monitor the data security practices of its vendor, AMCA.

71. As a direct and proximate result of Defendant's breach of the implied contracts, class members sustained damages as alleged herein.

72. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

73. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii)

submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

COUNT III
ILLINOIS PERSONAL INFORMATION PROTECTION ACT
NOTICE OF BREACH
(Illinois sub-class only)

74. Plaintiff realleges and incorporates by reference all preceding allegations.

75. Defendant is required to accurately notify Plaintiff and Class Members if Defendant becomes aware of a breach of its data security system (that was reasonably likely to have caused misuse of Plaintiff's and Class Members' Most Sensitive Personal Information) in the most expedient time possible and without unreasonable delay under 815 Ill. Comp. Stat. 5

76. Defendant is a Data Collector business that owns or licenses computerized data that includes personal information as defined by 815 Ill. Comp. Stat. 530/5.

77. Plaintiff and Class Members' Most Sensitive Personal Information (e.g., Social Security numbers) included Medical information and Personal information as defined under 815 Ill. Comp. Stat. 530/5.

78. Because Defendant was or should have been aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiff's and Class Members' Most Sensitive Personal Information, Defendant had an obligation to disclose the data breach in "the most expedient time possible and without unreasonable delay" as mandated in 815 Ill. Comp. Stat. 530/10.

79. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated 815 Ill. Comp. Stat. 530/10.

80. As a direct and proximate result of Defendant's violations of 815 Ill. Comp. Stat. 530/10, Plaintiff and Class Members suffered damages, as described above.

81. Plaintiff and Class Members seek relief under 815 Ill. Comp. Stat. 530/20 and 815 Ill. Comp. Stat. 505/1, 505/2z, 505/10a, including, actual damages, punitive damages, broad equitable relief, and attorneys' fees and costs.

COUNT IV

ILLINOIS PERSONAL INFORMATION PROTECTION ACT AND CONSUMER FRAUD AND DECEPTIVE BUSINESS PROTECTION ACT
(Illinois sub-class only)

82. Plaintiff realleges and incorporates by reference all preceding allegations.

83. Defendant is a Data Collector business that for any purpose, handles, collects, disseminates, and otherwise, deals with nonpublic personal information, as defined by 815 Ill. Comp. Stat. 530/5.

84. Plaintiff's and Class Members' Most Sensitive Personal Information (e.g., Social Security numbers, medical treatment billing history) included information that qualified as "Medical information" and "Personal information" as those terms are defined under 815 Ill. Comp. Stat. 530/5.

85. The Data Breach qualified as a "breach of the security of the system data" or "breach" as those terms are defined in 815 Ill. Comp. Stat. 530/5.

86. Defendant failed to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure" as required under 815 Ill. Comp. Stat. 530/45(a).

87. Plaintiff and Class Members seek relief under 815 Ill. Comp. Stat. 530/20 and 815 Ill. Comp. Stat. 505/1, 505/2z, 505/10a, including, actual damages, punitive damages, broad equitable relief, and attorneys' fees and costs.

COUNT V
NEGLIGENCE PER SE

88. Plaintiff realleges and incorporates by reference all preceding allegations.

89. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Most Sensitive Personal Information.

90. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Most Sensitive Personal Information.

91. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Most Sensitive Personal Information.

92. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), Gramm- Leach-Bliley Act (15 U.S.C. § 6801), and Illinois Personal Information Privacy Act (815 Ill. Comp. Stat. 530/1 *et seq.*) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Most Sensitive Personal Information.

93. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

94. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

95. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Most Sensitive Personal Information.

96. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

RELIEF REQUESTED

97. Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendant including the following:

a. Determining that this matter may proceed as a class action and certifying the classes asserted herein;

b. Appointing Plaintiff as representative of each of the classes and Plaintiff's counsel as class counsel;

c. An award to Plaintiff and the Class of compensatory and consequential damages;

d. Injunctive relief requiring Defendant to, e.g.,: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members;

e. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

f. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

g. Such other or further relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

ERICKSON J. OCASIO, individually and on behalf of all others similarly situated,

By: /s/ *Rusty Payton*
Rusty Payton

Rusty A. Payton
Payton Legal Group LLC
20 North Clark Street
Suite 3300
Chicago, Illinois 60602
(773) 682-5210
(773) 787-1550 (facsimile)
info@payton.legal

William B. Federman
Federman & Sherwood
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
Pro Hac Vice Admission to be sought